REMARKS

In the Official Action mailed on **04 June 2009**, the Examiner reviewed claims 1-33. Examiner rejected claims 11-12, and 16-19 under 35 U.S.C. § 112. Examiner rejected claims 1-12, and 15-33 under 35 U.S.C. § 103(a) based on Yavatkar et al (U.S. Patent No. 6,735,702, hereinafter "Yavatkar"), and Wetherall (U.S. Patent No. 7,058,015, hereinafter "Wetherall").

Rejections under 35 U.S.C. § 112

Examiner rejected claims 11-12, and 16-19 under 35 U.S.C. § 112, stating that the following claim limitations lack sufficient antecedent basis:

- Claim 11 recites the limitation "the control center" at line 2 of the claim. Applicant has amended claim 11 so that "the control center" now reads "a control center."
- Claim 12 recites the limitation "the destination address" at line 4 of the claim. Applicant has amended claim 12 so that "the destination address" now reads "a destination address."
- Claim 15 recites the limitation "the victim destination address" at line 10 of the claim. Applicant has amended claim 15 so that "the victim destination address" now reads "a victim destination address."
- Claim 15 recites the limitation "the data center" at line 11 of the claim. Applicant has amended claim 15 so that "the data center" now reads "a data center."
- Claim 16 recites the limitation "the control center" at line 2 of the claim. Applicant has amended claim 16 so that "the control center" now reads "a control center."

- Claim 16 recites the limitation "the data center" at line 3 of the claim. This claim does not recited the limitation "the data center" and instead recites the limitation "the victim data center," which has antecedent basis in claim 15.
- Claim 17 recites the limitation "the control center" at line 2 of the claim. The limitation "the control center" has antecedent basis in claim 16.
- Claim 18 recites the limitation "the victim destination address" at line 3 of the claim. The limitation "the victim destination address" has antecedent basis in claim 15.
- Claim 19 recites the limitation "the destination address" at line 4 of the claim. Applicant has amended claim 19 so that "the destination address" now reads "a destination address."

Rejections under 35 U.S.C. § 103

Examiner rejected claims 1-12, and 15-33 under 35 U.S.C. § 103(a) based on Yavatkar and Wetherall. Applicant respectfully disagrees with this rejection. Neither Yavatkar nor Wetherall discloses aggregating statistical information of traffic flows from a source address and source port to a destination address and destination port, measured over different periods of time.

Yavatkar discloses two types of agents that are used together to detect attacks: "watchdog" agents and "bloodhound" agents. "Watchdog agents detect network attacks and bloodhound agents trace the source of attacks" (Yavatkar, C14:L20-21). Thus, "watchdog" agents are deployed at a node and "bloodhound" agents are initiated at the node. Moreover,

> The bloodhound agent determines which port is accepting the greatest proportion of attack traffic. In determining which port is accepting the greatest proportion of such traffic, bloodhound agent thus detects which link connected to the node is accepting and carrying the greatest proportion of such traffic.

Nothing within Yavatkar suggests or implies processing statistical information to determine the source of suspicious network traffic sent to the data center, where processing comprises aggregating statistical information of traffic flows from a source address and source port to a destination address and destination port, measured over different periods of time.

Because Yavatkar's "bloodhound" agents traverse only a single path, they are unable to detect network-wide attacks. Moreover, because Yavatkar's "bloodhound" agents continually move from node to node, these agents are unable to detect attacks over different time periods. That is, the "bloodhound" agents do not remain long enough at a node to collect such information.

Wetherall discloses "sensors" that are externally disposed at boundary entry points of different domains in the network (Wetherall, C3:L64-C4:L7). These sensors are located at routing devices and they collect:

> …destination information, allowing the amount of network traffic destined for various network nodes of interest be discernable; volume of data with specific destinations passing through a routing device; volume of data with specific source and destination address combinations, the types of traffic passing through a routing device, and characteristics of packets of data. Examples of "traffic type" include Web, DNS, Real Networks, Secure Web, Other TCP, Other UDP, ICMP, TCP packets with ACK set, TCP packets without SYN set, and so forth. Examples of "characteristics" include distribution of lengths of packet, distribution of Time to Live values, and so forth. (Wetherall, C4:L47-60).

However, the "sensors" in Wetherall do not aggregate information on traffic flows.

Wetherall discloses a "director" that can receive network traffic data as reported by the "sensors" (Wetherall, C7:L51-53). This "director" also includes an "analyzer" that "analyzes the network traffic data to determine if regulation/de-regulation actions need to be taken" (Wetherall, C7:54-56). However, the "analyzer" only attempts to determine whether the volume of traffic

at a boundary entry point has reached or fallen below a threshold (Wetherall, C7:L59-67), but does not perform aggregation on information of traffic flows.

In contrast, embodiments of the present invention involve processing statistical information to determine the source of suspicious network traffic sent to the data center. This processing comprises aggregating statistical information of traffic flows from a source address and source port to a destination address and destination port, measured over different periods of time. See instant application, P21:L21-30 and P6:L7-9. Because the system claimed in the present invention collects measurements over time (ranging from minutes to weeks), the system can be used to detect subtle attacks mounted slowly over time.

Such traffic-flow aggregation is not disclosed in the cited references. Yavatkar's "watchdog" and "bloodhound" agents are local in space as well as time, as are Wetherall's "sensors," which are not capable of performing such operation. Furthermore, Wetherall's "director" does not aggregate traffic flow data and only analyzes data at individual boundary entry points.

Accordingly, Applicant has amended independent claims 1, 15, 20, and 29 to clarify that embodiments of the present invention involve processing statistical information to determine the source of suspicious network traffic sent to the data center, where processing comprises aggregating statistical information of traffic flows from a source address and source port to a destination address and destination port, measured over different periods of time. Support for these amendments is found in instant application, P21:L21-30 and P6:L7-9. Applicant has also amended claim 20 so that "a the source" now reads "a source." No new matter has been added.

Hence, Applicant respectfully submits that independent claims 1, 15, 20, and 29 as presently amended are in condition for allowance. Applicant also submits that claims 2-14 and claim 33, which depend upon claim 1, claims 16-19, which depend upon claim 15, claims 21-28, which depend upon claim 20, claims

30-32, which depend upon claim 29, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By /Shun Yao/
Shun Yao
Registration No. 59,242

Date: 05 October 2009

Shun Yao
Park, Vaughan & Fleming LLP
2820 Fifth Street
Davis, CA 95618-7759
Tel: (530) 759-1667
Fax: (530) 759-1665
Email: shun@parklegal.com